WHAT SHOULD YOU DO IF YOU ARE A VICTIM OF IDENTITY THEFT?

Step 1. **Close any problem account**

Contact the credit card companies, banks or any other creditor to close the account that you know have been tampered with or opened fraudulently.

Step 2. **Contact the Credit Bureaus**

Contact the fraud department of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alter requires that creditors contact you before opening any new accounts or making any changes to your existing accounts. When you place a fraud alert on your credit file, all three bureaus are required by law to automatically send a credit report free of charge to you.

This "one-call" **Fraud Alert** will remain on your credit file for at least 90 days.

Step 3. **Contact the Fraud Department of each of your Creditors**

Make sure that each of your creditors are aware that an identity thief may have your account information. Ask each of your creditors to place a **"Fraud Alert"** on your account.

Step 4. **Promptly make a report with your local Police Department**

File a police report with your local police department, keep a copy for yourself and give a copy to your creditors and the credit bureaus.

District Attorney Michael D. O'Keefe
Cape & Islands District Attorney's Office
3231 Main Street, Barnstable, MA 02630
Phone: (508) 362-8113
Fax: (508) 362-8221

Cape & Islands District Attorney's Office

District Attorney Michael D. O'Keefe

IDENTITY THEFT

Don't let it happen to you!

Website: www.mass.gov/da/cape

District Attorney Michael D. O'Keefe suggests that you take these precautions to avoid becoming a victim

- Do not give your personal information, i.e. social security number, last four digits of social security number, mother's maiden name, to anyone unless you have initiated the contact and know who you are dealing with. Including banks and the IRS.
- Do not use obvious passwords, include letters (uppercase and lowercase, numbers and symbols)
- Do not respond to phone, e-mail or mail solicitations from businesses attempting to confirm your personal information in exchange for an offer of something that seems too good to be true. Ask for a number to call back.
- Do not send or give authorization numbers off the back of pre-paid credit cards to anyone posing as a relative (grandparent scam) or friend asking for money. Ask for a number to call them back.
- Destroy, shred or tear up any credit application or any other documents with your personal information before you throw them away.
- Review your monthly statements and report any unauthorized charges. If banking online, set up alerts for unusual charges, purchases or withdrawals. Have your balance sent to you weekly.
- Order yearly credit reports and check your credit history for fraudulent activity. By law the credit bureaus are required to send you an annual report at no cost, if you request one.

EQUIFAX : www.equifax.com
800-525-6285

TRANSUNION: www.transunion.com
800-680-7289

EXPERIAN: www.experian.com
888-397-3742

Online: www.annualcreditreport.com
Mail: Annual Credit Report Request Services,
P.O. Box 105281, Atlanta, GA 30348-5281
Phone: 1-877-322-8228

Other Resources:
Elder Services of Cape Cod & Islands
1-800-244-4630, 508-394-4630

Secretary of State: Securities Division: Fraud
1-800-269-5428

Attorney General Office: Elder Hotline
1-888-AG-ELDER